

| | | | |
|-------------------------------|------------------------|---------------------|--|
| Notice of Allowability | Application No. | Applicant(s) | |
| | 09/720,353 | NOLTE, MICHAEL | |
| | Examiner | Art Unit | |
| | Peter Poltorak | 2134 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to communication received on 10/19/06.
2. ☒ The allowed claim(s) is/are 2-17.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☒ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|--|
| <ol style="list-style-type: none"> 1. <input type="checkbox"/> Notice of References Cited (PTO-892) 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) 3. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____ 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit of Biological Material | <ol style="list-style-type: none"> 5. <input type="checkbox"/> Notice of Informal Patent Application 6. <input type="checkbox"/> Interview Summary (PTO-413), Paper No./Mail Date _____ 7. <input type="checkbox"/> Examiner's Amendment/Comment 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance 9. <input type="checkbox"/> Other _____ |
|---|--|

DETAILED ACTION

1. This Office Action is in response to communication received on 10/19/06.
2. Claims 2-17 are allowed.

Examiner's Statement of Reasons for Allowance

The following is a statement of reasons for the indication of allowable subject matter.

3. Applicant's invention relates to signing of messages using signing keys and signature verification using check keys.
4. The independent claims 9 and 11 identify the uniquely distinct features: signature verification involves three parties: control center, sender and receiver, wherein "the sender, the receiver, and the control center are individual and separate one from the others". More specifically, a shared key stored in the control center and the receiver are ran with a sequence number trough a one way function to produce the signing/check keys. The signing key is sent to the sender that signs a message and forwards it with the signature to a receiver that verifies the signature.
5. The closest prior art, Hoffmann et al. (U.S. Patent No. 5608800), teach signature verification, wherein a transmitter that (functions as a control center and a sender) shares a common main key with a receiver. However, Hoffman et al.'s system involves only two individual and separate parties: a transmitter and a receiver. Hoffman et al. do not disclose that "the control center, the receiver, and the sender are individual and separate one from the other" as required by the independent claims 9 and 11.

Art Unit: 2134

6. The examiner also considered three parties protocol, specifically Kerberos (version 4) that teaches a control center (Authentication Server), a sender (client) and a receiver (server). However, in Kerberos scheme the sender uses a signing key (session key) to encrypt a message (ticket) rather than forming a signature and the receiver check key (that corresponds to the signing key) together with a sequence number is not used to calculate the signature for comparison to the signature of the message. Instead the check key simply decrypts the message (*Stallings, pg. 328-340*).

Kerberos, does not disclose that "the check key and determined sequence number being used to form a calculated signature for comparison to the signature of the data message block" as required by the independent claims 9 and 11.

7. The prior art, fails to anticipate or fairly suggest the limitation of applicant's independent claims (interpreted in light of the specification), in such a manner that a rejection under 35 U.S.C. 102 or 103 would be proper. As a result the claimed invention is considered to be in condition for allowance as being novel and non-obvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on statement of Reasons for Allowance".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-

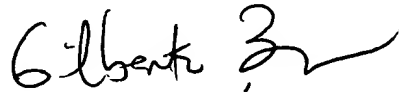
Art Unit: 2134

3840. The examiner can normally be reached from Monday through Thursday from 9:00 until 5:00, and every other Friday from 9:00 until 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis Jacques can be reached on (571)272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (571) 272-1600.



11/20/06



GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100